# HODGE GROUPS OF CERTAIN SUPERELLIPTIC JACOBIANS II

JIANGWEI XUE

## 1. INTRODUCTION

Throughout this paper $\mathbf{C}$ is the field of complex numbers, $K \subseteq \mathbf{C}$ is a subfield of $\mathbf{C}$, $f(x) \in K[x]$ a polynomial without multiple roots and of degree $n \geq 4$. Let $p \in \mathbf{N}$ be a prime that does not divide $n$ and $q = p^r \in \mathbf{N}$ an integral power of $p$. We write $C_{f,q}$ for the superelliptic $K$-curve $y^q = f(x)$, and $J(C_{f,q})$ for the Jacobian of $C_{f,q}$. By definition, $C_{f,q}$ is the smooth projective model of the affine curve $y^q = f(x)$. The Jacobian $J(C_{f,q})$ is an abelian variety over $K$ of dimension

$$\dim J(C_{f,q}) = g(C_{f,q}) = \frac{(n-1)(q-1)}{2}.$$

If $q > p$, the map

$$C_{f,q} \to C_{f,q/p}, \quad (x, y) \mapsto (x, y^p)$$

induces by Albanese fuctoriality a surjective $K$-map between the Jacobians $J(C_{f,q}) \to J(C_{f,q/p})$. We write $J^{(f,q)}$ for the identity component of the kernel. If $q = p$, we set $J^{(f,p)} = J(C_{f,p})$. It is follows easily that $J^{(f,q)}$ is an abelian variety over $K$ of dimension $(n-1)\varphi(q)/2$, where $\varphi$ denotes the Euler $\varphi$-function. Moreover, $J(C_{f,q})$ is $K$-isogenous to the product $\prod_{i=1}^{r} J^{(f,p^i)}$(See [15]).

Since $K \subseteq \mathbf{C}$, we may view $J^{(f,q)}$ as a complex abelian variety. We refer to [5], [10, Sect. 6.6.1 and 6.6.2] for the definition and basic properties of the Hodge group (aka special Mumford–Tate group). In [9], assuming that $n > q$ and some other conditions on $n, q$ and $f(x)$, the authors showed that the (reductive $\mathbf{Q}$-algebraic connected) Hodge group of $J^{(f,q)}$ coincides with the largest $\mathbf{Q}$-algebraic subgroup of $\mathrm{GL}(\mathrm{H}^1(J^{(f,q)}, \mathbf{Q}))$ that's "cut out" by the induced polarization from the canonical principal polarization of $J(C_{f,q})$ and the endomorphism ring of $J^{(f,q)}$. Notice that when $q = 2$ (i.e., in the hyperelliptic case) this group was completely determined in [12] (when $f(x)$ has "large" Galois group). In this paper, we study some additional properties of $J^{(f,q)}$ which will allow us to extend the result to the case $n < q$ as well. This case is necessary in order to treat the infinite towers of superelliptic jacobians, which, in turn, are useful for the study of the ranks of Mordell-Weil groups in infinite towers of function fields (See [6]).

To state our main result, we make explicit the endomorphism ring and the polarization mentioned above. Let $X$ be an abelian variety over $\bar{K}$. We write $\mathrm{End}(X)$ for the ring of all its $\bar{K}$-endomorphisms and $\mathrm{End}^0(X)$ for the endomorphism algebra $\mathrm{End}(X) \otimes_{\mathbf{Z}} \mathbf{Q}$. In a series of papers [11, 13, 14, 15], Yuri Zarhin discussed the structure of $\mathrm{End}^0(J(C_{f,q}))$, assuming that $n \geq 5$ and the Galois group $\mathrm{Gal}(f)$ of $f(x)$ over $K$ is, at least, doubly transitive. Here $\mathrm{Gal}(f) \subseteq \mathbf{S}_n$ is viewed as a permutation group on the roots of $f(x)$. It is well known that $f(x)$ is irreducible

over $K$ if and only if $\mathrm{Gal}(f)$ acts transitively on the roots. For the sake of simplicity let's assume that $K$ contains a primitive $q$-th root of unity $\zeta_q$. The curve $C_{f,q} : y^q = f(x)$ admits the obvious periodic automorphism

$$\delta_q : C_{f,q} \to C_{f,q}, \quad (x, y) \mapsto (x, \zeta_q y).$$

By an abuse of notation, we also write $\delta_q$ for the induced automorphism of $J(C_{f,q})$. The subvariety $J^{(f,q)}$ is $\delta_q$-invariant and we have an embedding

$$\mathbf{Z}[\zeta_q] \hookrightarrow \mathrm{End}(J^{(f,q)}), \quad \zeta_q \mapsto \delta_q.$$

In particular, the $q$-th cyclotomic filed $E := \mathbf{Q}(\zeta_q)$ is contained in $\mathrm{End}^0(J^{(f,q)})$. Zarhin showed ([11, 15, 17]) that $\mathrm{End}(J^{(f,q)})$ is isomorphic to $\mathbf{Z}[\zeta_q]$ if either $\mathrm{Gal}(f)$ coincides with the full symmetric group $\mathbf{S}_n$, $n \geq 4$ and $p \geq 3$, or $\mathrm{Gal}(f)$ coincides with the alternating group $\mathbf{A}_n$ (or $\mathbf{S}_n$), and $n \geq 5$. This result has also been extended to the case $\mathrm{Gal}(f) = \mathbf{S}_n$ or $\mathbf{A}_n$, $n \geq 5$ and $p \mid n$ in [7].

The first rational homology group $\mathrm{H}_1(J^{(f,q)}, \mathbf{Q})$ carries a natural structure of $E$-vector space of dimension

$$\dim_E \mathrm{H}_1(J^{(f,q)}, \mathbf{Q}) = \frac{\dim_{\mathbf{Q}} \mathrm{H}_1(J^{(f,q)}, \mathbf{Q})}{[E : \mathbf{Q}]} = \frac{2\dim J^{(f,q)}}{[E : \mathbf{Q}]} = \frac{(n-1)\varphi(q)}{\varphi(q)} = n - 1.$$

Notice that if $q > 2$, then $E$ is a CM field with complex conjugation $e \mapsto \bar{e}$. Let

$$E^+ = \{e \in \mathbf{Q}(\zeta_q) \mid \bar{e} = e\}$$

be the maximal totally real subfield of $E$ and let

$$E_- = \{e \in \mathbf{Q}(\zeta_q) \mid \bar{e} = -e\}.$$

The canonical principal polarization on $J(C_{f,q})$ induces a polarization on $J^{(f,q)}$, which gives rise to a nondegenerate $E$-sesquilinear Hermitian form ([9])

$$\phi_q : \mathrm{H}_1(J^{(f,q)}, \mathbf{Q}) \times \mathrm{H}_1(J^{(f,q)}, \mathbf{Q}) \to E.$$

We write $\mathrm{U}(\mathrm{H}_1(J^{(f,q)}, \mathbf{Q}), \phi_q)$ for the unitary group of $\phi_q$ of the $\mathbf{Q}(\zeta_q)$-vector space $\mathrm{H}_1(J^{(f,q)}, \mathbf{Q})$, viewed as an $\mathbf{Q}$-algebraic subgroup of $\mathrm{GL}(\mathrm{H}_1(J^{(f,q)}, \mathbf{Q}))$ (via Weil's restriction of scalars from $E^+$ to $\mathbf{Q}$ ([5])). Since the Hodge group respects the polarization and commutes with endomorphisms of $J^{(f,q)}$,

$$\mathrm{Hdg}(J^{(f,q)}) \subset \mathrm{U}(\mathrm{H}_1(J^{(f,q)}, \mathbf{Q}), \phi_q).$$

If $\mathrm{End}^0(J^{(f,q)}) = E$, then $\mathrm{U}(\mathrm{H}_1(J^{(f,q)}, \mathbf{Q}), \phi_q)$ is the largest connected reductive $\mathbf{Q}$-algebraic subgroup of $\mathrm{GL}(\mathrm{H}_1(J^{(f,q)}, \mathbf{Q}))$ that both respects the polarization and commutes with endomorphisms of $J^{(f,q)}$.

The following theorem is a natural extension of [9, Theorem 0.1].

**Theorem 1.** *Suppose that $n \geq 4$ and $p$ is a prime that does not divide $n$. Let $f(x) \in \mathbf{C}[x]$ be a degree $n$ polynomial without multiple roots. Let $r$ be a positive integer and $q = p^r$. Suppose that there exists a subfield $K$ of $\mathbf{C}$ that contains all the coefficients of $f(x)$. Let us assume that $f(x)$ is irreducible over $K$ and the Galois group $\mathrm{Gal}(f)$ of $f(x)$ over $K$ is either $\mathbf{S}_n$ or $\mathbf{A}_n$. Assume additionally that either $n \geq 5$ or $n = 4$ and $\mathrm{Gal}(f) = \mathbf{S}_4$.*

*Suppose that one of the following three conditions holds:*

(A) *$n = q + 1$;*
(B) *$p$ is odd and $n \not\equiv 1 \mod q$;*
(C) *$p = 2$, $n \not\equiv 1 \mod q$ and $n \not\equiv q - 1 \mod 2q$.*

*Then* $\mathrm{Hdg}(J^{(f,q)}) = \mathrm{U}(\mathrm{H}_1(J^{(f,q)}, \mathbf{Q}), \phi_q)$.

**Corollary 2.** *Corollary 0.3, Theorem 4.2 and Theorem 4.3 of* [9] *all hold without the assumption that* $n > q$.

**Remark 3.** We assume that $n < q$ throughout the rest of the paper since the case $n > q$ has already been treated in [9].

**Remark 4.** Since both $\mathrm{Hdg}(J^{(f,q)})$ and $\mathrm{U}(\mathrm{H}_1(J^{(f,q)}, \mathbf{Q}), \phi_q)$ are connected $\mathbf{Q}$-algebraic groups, to prove Theorem 1, it suffices to show that

$$\dim \mathrm{Hdg}(J^{(f,q)}) \geq \dim \mathrm{U}(\mathrm{H}_1(J^{(f,q)}, \mathbf{Q}), \phi_q).$$

It is known that

$$\dim \mathrm{U}(\mathrm{H}_1(J^{(f,q)}, \mathbf{Q}), \phi_q) = \dim_{\mathbf{Q}} E^+ \cdot \left(\dim_E \mathrm{H}_1(J^{(f,q)}, \mathbf{Q})\right)^2.$$

Let hdg be the $\mathbf{Q}$-Lie algebra of $\mathrm{Hdg}(J^{(f,q)})$. It is a reductive $\mathbf{Q}$-Lie subalgebra of $\mathrm{End}_{\mathbf{Q}}\big(\mathrm{H}_1(J^{(f,q)}, \mathbf{Q})\big)$, and thus splits into a direct sum

$$\mathrm{hdg} = \mathfrak{c} \oplus \mathrm{hdg}^{ss},$$

of its center $\mathfrak{c}$ and the semisimple part $\mathrm{hdg}^{ss} = [\mathrm{hdg}, \mathrm{hdg}]$. By [8, Theorem 1.3], if $\mathrm{Gal}(f) = \mathbf{S}_n$ and $n \geq 4$, or $\mathrm{Gal}(f) = \mathbf{A}_n$ and $n \geq 5$, the center $\mathfrak{c}$ coincides with $E_-$. Notice that

$$\dim_{\mathbf{Q}} E_- = \dim_{\mathbf{Q}} E^+ = [E : \mathbf{Q}]/2.$$

Theorem 1 follows if we show that

$$\dim_{\mathbf{Q}} \mathrm{hdg}^{ss} \geq \frac{1}{2}[E : \mathbf{Q}]\big((\dim_E \mathrm{H}_1(J^{(f,q)}, \mathbf{Q}))^2 - 1\big). \tag{1}$$

The paper is organized as follows. In section 2 we study the Galois actions on certain vector spaces. In section 3 we recall some facts about the Hodge Lie algebra hdg. The proof of Theorem 1 is given at the end of section 3 except a key arithmetic lemma, which is proven in Section 4.

## 2. Galois Actions

Throughout this section, let $E$ be a field that is a finite Galois extension of $\mathbf{Q}$ with Galois group $G$. Let $V$ be a $E$-vector space of finite dimension. We write $V_{\mathbf{Q}}$ for the underlying $\mathbf{Q}$-vector space of $V$, and $V_{\mathbf{C}}$ for the $\mathbf{C}$-vector space $V \otimes_{\mathbf{Q}} \mathbf{C} = V_{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{C}$. Let $\mathrm{Aut}(\mathbf{C})$ be the group of all automorphisms of $\mathbf{C}$. It act semilinearly on $V_{\mathbf{C}} = V \otimes_{\mathbf{Q}} \mathbf{C}$ through the second factor. More explicitly, $\forall \kappa \in \mathrm{Aut}(\mathbf{C}), v \otimes z \in V \otimes_{\mathbf{Q}} \mathbf{C}$, we define $\kappa(v \otimes z) := v \otimes \kappa(z)$. It follows that $\forall x \in V \otimes_{\mathbf{Q}} \mathbf{C}$ and $c \in \mathbf{C}$, $\kappa(cx) = \kappa(c)x$. On the other hand, $E$ acts on $V_{\mathbf{C}} = V \otimes_{\mathbf{Q}} \mathbf{C}$ through its first factor. It follows that $V_{\mathbf{C}}$ is a free $E \otimes_{\mathbf{Q}} \mathbf{C}$ module of rank $\dim_E V$, and the action of $E = E \otimes 1 \subseteq E \otimes_{\mathbf{Q}} \mathbf{C}$ commutes with that of $\mathrm{Aut}(\mathbf{C})$. In other words,

$$\kappa((e \otimes 1)x) = (e \otimes 1)\kappa(x), \quad \forall \kappa \in \mathrm{Aut}(\mathbf{C}), e \in E, \text{ and } x \in V_{\mathbf{C}}.$$

Let's fix an embedding $E \hookrightarrow \mathbf{C}$. This allows us to identify each Galois automorphism $\sigma : E \to E$ with the embedding $\sigma : E \to E \subset \mathbf{C}$ of $E$ into $\mathbf{C}$. It is well known that

$$E_{\mathbf{C}} := \mathrm{E} \otimes_{\mathbf{Q}} \mathbf{C} = \bigoplus_{\sigma \in G} E \otimes_{E,\sigma} \mathbf{C} = \bigoplus_{\sigma \in G} \mathbf{C}_\sigma, \text{ where } \mathbf{C}_\sigma := E \otimes_{E,\sigma} \mathbf{C}.$$

So every $E_{\mathbf{C}}$ module $W$ splits as a direct sum $W = \oplus_{\sigma\in G} W_\sigma$, where

$$W_\sigma := \mathbf{C}_\sigma W = \{w \in W \mid (e\otimes 1)w = \sigma(e)w, \forall e \in E\}.$$

In particular, $V_{\mathbf{C}} = \oplus_{\sigma\in G} V_\sigma$, and each $V_\sigma$ is a $\mathbf{C}$-vector space of dimension $\dim_E V$. For each $\sigma \in G$, let $P_\sigma : V_{\mathbf{C}} \to V_\sigma$ be the $\mathbf{C}$-linear projection map from $V_{\mathbf{C}}$ to the summand $V_\sigma$. Similarly, for each pair $\sigma \neq \tau$, we write $P_{\sigma,\tau} = P_\sigma \oplus P_\tau : V_{\mathbf{C}} \to V_\sigma \oplus V_\tau$ for the projection map onto this pair of summands.

We claim that $\mathrm{Aut}(\mathbf{C})$ permutes the set $\{V_\sigma \mid \sigma \in G\}$, and the action factors through the canonical restriction

$$\mathrm{Aut}(\mathbf{C}) \twoheadrightarrow G, \quad \kappa \mapsto \kappa\mid_E .$$

Indeed, for all $\kappa \in \mathrm{Aut}(\mathbf{C}), e \in E$ and $x_\sigma \in V_\sigma$,

$$(e\otimes 1)\kappa(x_\sigma) = \kappa((e\otimes 1)x_\sigma) = \kappa(\sigma(e)x_\sigma) = \kappa(\sigma(e))\kappa(x_\sigma) = \kappa\sigma(e)\kappa(x_\sigma).$$

Clearly $\kappa\sigma(e) = ((\kappa\mid_E)\sigma)(e)$. By an abuse of notation, we write $\kappa$ for the restriction $\kappa\mid_E$. So it follows that $\kappa(x_\sigma) \in V_{\kappa\sigma}$, and thus $\kappa(V_\sigma) = V_{\kappa\sigma}$ for all $\kappa \in \mathrm{Aut}(\mathbf{C})$ and $\sigma \in G$.

Let us define an action of $\mathrm{Aut}(\mathbf{C})$ on the set of projection $\mathcal{P} = \{P_\sigma \mid \sigma \in G\}$ by

$$\kappa_* P_\sigma := \kappa \circ P_\sigma \circ \kappa^{-1}.$$

Then for any element $\sum x_\sigma \in \oplus_{\sigma\in G} V_\sigma = V_{\mathbf{C}}$ and $P_\tau \in \mathcal{P}$,

$$(\kappa_* P_\tau)(\sum x_\sigma) = \kappa \circ P_\tau \left(\sum \kappa^{-1}(x_\sigma)\right) = \kappa(\kappa^{-1}(x_{\kappa\tau})) = x_{\kappa\tau},$$

where all summations runs through $\sigma \in G$, and we used the fact that $\kappa^{-1}(x_\sigma)$ belongs to $V_\tau$ if and only if $\sigma = \kappa\tau$. Therefore,

$$\kappa_* P_\sigma = P_{\kappa\sigma}.$$

Clearly $\mathrm{Aut}(\mathbf{C})$ acts transitively on $\mathcal{P}$. Since $P_{\sigma,\tau} = P_\sigma \oplus P_\tau$, we have similarly an action of $\mathrm{Aut}(\mathbf{C})$ on the set $\mathcal{PP} := \{P_{\sigma,\tau} \mid (\sigma,\tau) \in G^2, \sigma \neq \tau\}$ by

$$\kappa_* P_{\sigma,\tau} = \kappa \circ P_{\sigma,\tau} \circ \kappa^{-1} = P_{\kappa\sigma,\kappa\tau}.$$

The $\mathrm{Aut}(\mathbf{C})$-orbit $O_{\sigma,\tau}$ of each $P_{\sigma,\tau} \in \mathcal{PP}$ consists of all elements of the form $P_{\kappa\sigma,\kappa\tau}$ with $\kappa \in G$.

**Lemma 5.** *Let $W_{\mathbf{Q}} \subseteq V_{\mathbf{Q}}$ be any $\mathbf{Q}$-subspace of $V_{\mathbf{Q}}$, and $W_{\mathbf{C}} := W_{\mathbf{Q}} \otimes_{\mathbf{Q}} \mathbf{C} \subseteq V_{\mathbf{C}}$ be its complexification.*

(i) *If there exists $\sigma_0 \in G$ such that $P_{\sigma_0}(W_{\mathbf{C}}) = V_{\sigma_0}$, then $P_\sigma(W_{\mathbf{C}}) = V_\sigma$ for all $\sigma \in G$.*
(ii) *If there exists a pair $(\sigma_0, \tau_0) \in G^2$ with $\sigma_0 \neq \tau_0$ such that $P_{\sigma_0,\tau_0}(W_{\mathbf{C}}) = V_{\sigma_0} \oplus V_{\tau_0}$, then $P_{\sigma,\tau}(W_{\mathbf{C}}) = V_\sigma \oplus V_\tau$ for all $P_{\sigma,\tau} \in O_{\sigma_0,\tau_0}$.*

*Proof.* Clearly, $W_{\mathbf{C}}$ is $\mathrm{Aut}(\mathbf{C})$-invariant. For each $\sigma \in G$, let us choose $\kappa \in \mathrm{Aut}(\mathbf{C})$ such that $\sigma = \kappa\sigma_0$. Then

$$P_\sigma(W_{\mathbf{C}}) = (\kappa_* P_{\sigma_0})(W_{\mathbf{C}}) = \kappa \circ P_{\sigma_0} \circ \kappa^{-1}(W_{\mathbf{C}}) = \kappa \circ P_{\sigma_0}(W_{\mathbf{C}}) = \kappa(V_{\sigma_0}) = V_\sigma.$$

This proves part (i). Similarly, suppose that $P_{\sigma_0,\tau_0}(W_{\mathbf{C}}) = V_{\sigma_0} \oplus V_{\tau_0}$. For all $P_{\sigma,\tau} \in O_{\sigma_0,\tau_0}$, there exists $\kappa \in \mathrm{Aut}(\mathbf{C})$ such that $\sigma = \kappa\sigma_0$ and $\tau = \kappa\tau_0$. So we have

$$\begin{aligned} P_{\sigma,\tau}(W_{\mathbf{C}}) &= (\kappa_* P_{\sigma_0,\tau_0})(W_{\mathbf{C}}) = \kappa \circ P_{\sigma_0,\tau_0} \circ \kappa^{-1}(W_{\mathbf{C}}) = \kappa \circ P_{\sigma_0,\tau_0}(W_{\mathbf{C}}) \\ &= \kappa(V_{\sigma_0} \oplus V_{\tau_0}) = \kappa(V_{\sigma_0}) \oplus \kappa(V_{\tau_0}) = V_\sigma \oplus V_\tau, \end{aligned}$$

and part (ii) follows. $\square$

Let $R$ be a commutative ring with unity, and $N$ be a free $R$-module of finite rank. We write $\mathrm{Tr}_R : \mathrm{End}_R(N) \to R$ for the trace map, and

$$\mathfrak{sl}_R(N) := \{g \in \mathrm{End}_R(N) \mid \mathrm{Tr}_R(g) = 0\}$$

for the $R$-Lie algebra of traceless endomorphisms of $N$. It is well-known that

$$\mathfrak{sl}_E(V) \otimes_{\mathbf{Q}} \mathbf{C} = \mathfrak{sl}_{E_{\mathbf{C}}}(V_{\mathbf{C}}) = \mathfrak{sl}_{E_{\mathbf{C}}}(\oplus_{\sigma \in G} V_\sigma) = \bigoplus_{\sigma \in G} \mathfrak{sl}_{\mathbf{C}}(V_\sigma).$$

We will denote the projection map $\mathfrak{sl}_E(V) \otimes_{\mathbf{Q}} \mathbf{C} \to \mathfrak{sl}_{\mathbf{C}}(V_\sigma)$ again by $P_\sigma$, and similarly for $P_{\sigma,\tau}$. Clearly, each $\mathfrak{sl}_{\mathbf{C}}(V_\sigma)$ has $\mathbf{C}$-dimension $(\dim_E V)^2 - 1$.

For the rest of the section, we assume additionally that $E$ is a CM-field. For any $\sigma \in G$, let $\bar{\sigma} : E \to E$ be the complex conjugation of $\sigma$. In other words, $\bar{\sigma}$ is the composition $E \xrightarrow{\sigma} E \to E$, where the second arrow stands for the complex conjugation map $e \mapsto \bar{e}$.

**Lemma 6.** *Let $\mathfrak{k}$ be a semisimple $\mathbf{Q}$-Lie subalgebra of $\mathfrak{sl}_E(V)$, and $\mathfrak{k}_{\mathbf{C}} := \mathfrak{k} \otimes_{\mathbf{Q}} \mathbf{C}$ be its complexification. Suppose that the following two conditions holds:*

(I) *there exists $\sigma_0 \in G$ such that $P_{\sigma_0}(\mathfrak{k}_{\mathbf{C}}) = \mathfrak{sl}_{\mathbf{C}}(V_{\sigma_0})$;*
(II) *For each pair $(\sigma, \tau) \in G^2$ with $\sigma \neq \tau$ and $\sigma \neq \bar{\tau}$, there exists $P_{\sigma_0,\tau_0} \in O_{\sigma,\tau}$ such $P_{\sigma_0,\tau_0(\mathfrak{k}_{\mathbf{C}})} = \mathfrak{sl}_{\mathbf{C}}(V_{\sigma_0}) \oplus \mathfrak{sl}_{\mathbf{C}}(V_{\tau_0})$.*

*Then*

$$\dim_{\mathbf{Q}} \mathfrak{k} \geq \frac{1}{2}[E : \mathbf{Q}] \left((\dim_E V)^2 - 1\right).$$

*Proof.* Applying Lemma 5 with $\mathfrak{k}$ in place of $W$ and $\mathfrak{sl}_E(V)$ in place of $V$, we see that

$$P_\sigma(\mathfrak{k}_{\mathbf{C}}) = \mathfrak{sl}_{\mathbf{C}}(V_\sigma), \quad \forall \sigma \in G;$$
$$P_{\sigma,\tau}(\mathfrak{k}_{\mathbf{C}}) = \mathfrak{sl}_{\mathbf{C}}(V_\sigma) \oplus \mathfrak{sl}_{\mathbf{C}}(V_\tau), \quad \forall (\sigma, \tau) \in G^2 \text{ with } \sigma \neq \tau \text{ and } \sigma \neq \bar{\tau}.$$

Let us fix a CM-type $\Phi$ of $E$. By definition, $\Phi$ is a maximal subset of $G = \mathrm{Hom}(E, \mathbf{C})$ such that no two elements of $\Phi$ are complex conjugate to each other. Clearly, $|\Phi| = [E : \mathbf{Q}]/2$, and

$$\dim_{\mathbf{C}} \Big( \bigoplus_{\sigma \in \Phi} \mathfrak{sl}_{\mathbf{C}}(V_\sigma) \Big) = \frac{1}{2}[E : \mathbf{Q}](\dim_E(V)^2 - 1).$$

Let $\mathfrak{k}'_{\mathbf{C}}$ be the projection of $\mathfrak{k}_{\mathbf{C}}$ on $\oplus_{\sigma \in \Phi} \mathfrak{sl}_{\mathbf{C}}(V_\sigma)$. It follows that the projection $\mathfrak{k}'_{\mathbf{C}} \to \mathfrak{sl}_{\mathbf{C}}(V_\sigma)$ is surjective for all $\sigma \in \Phi$, and $\mathfrak{k}'_{\mathbf{C}}$ also projects surjectively onto $\mathfrak{sl}_{\mathbf{C}}(V_\sigma) \oplus \mathfrak{sl}_{\mathbf{C}}(V_\tau)$ for all distinct pairs $\sigma, \tau \in \Phi$. Therefore, $\mathfrak{k}'_{\mathbf{C}} = \oplus_{\sigma \in \Phi} \mathfrak{sl}_{\mathbf{C}}(V_\sigma)$ by the Lemma on pp.790-791 of [4]. In particular, we get

$$\dim_{\mathbf{Q}} \mathfrak{k} = \dim_{\mathbf{C}} \mathfrak{k}_{\mathbf{C}} \geq \dim_{\mathbf{C}} \mathfrak{k}'_{\mathbf{C}} = \frac{1}{2}[E : \mathbf{Q}] \left((\dim_E V)^2 - 1\right).$$

□

In the next section, we will show that our semisimple part of Hodge Lie algebra $\mathrm{hdg}^{ss} = [\mathrm{hdg}, \mathrm{hdg}]$ satisfies (I) and (II) of Lemma 6 and thus prove our Main Theorem.

## 3. The Hodge Lie algebra

We keep all notation and assumptions of the previous sections. More specifically, $\zeta_q$ is a primitive $q$-th root of unity, $E = \mathbf{Q}(\zeta_q)$ and $G = \mathrm{Gal}(E/\mathbf{Q}) = (\mathbf{Z}/q\mathbf{Z})^*$, where each $a \in (\mathbf{Z}/q\mathbf{Z})^*$ maps $\zeta_q$ to $\zeta_q^a$. In order to simplify the notation, we write $X$ for the abelian variety $J^{(f,q)}$, and $V$ for its first rational homology group $\mathrm{H}_1(X, \mathbf{Q})$. In addition, we assume that $\mathrm{End}^0(X) = E$.

Recall that $E_{\mathbf{C}} = E \otimes_{\mathbf{Q}} \mathbf{C}$. Let $\mathrm{Lie}(X)$ be the complex tangent space to the origin of $X$. By functoriality, $E$ acts on $\mathrm{Lie}(X)$ and provides $\mathrm{Lie}(X)$ with a natural structure of $E_{\mathbf{C}}$-module. Therefore, $\mathrm{Lie}(X)$ splits into a direct sum

$$\mathrm{Lie}(X) = \oplus_{a \in G} \mathrm{Lie}(X)_a.$$

where $\mathrm{Lie}(X)_a := \{x \in \mathrm{Lie}(X) \mid (\zeta_q \otimes 1)x = \zeta_q^a x\}$. Let us put $n_a = \dim_{\mathbf{C}} \mathrm{Lie}(X)_a$. It is known that $n_a = [na/q]$ (see [15, 16]), where $[x]$ is the maximal integer that's less or equal to $x$, and we take the representative $1 \leq a \leq q-1$.

**Remark 7.** By [9, Proposition 2,1, 2.2], the assumptions (A)(B)(C) of Theorem 1 guarantee that there exists an integer $a$ such that

$$1 \leq a \leq q-1, \quad \gcd(a, p) = 1$$

and the integers $[na/q]$ and $\dim_E V = n-1$ are relative prime. We note that the conditions (A)(B)(C) of Theorem 1 are equivalent to the conditions (A)(B)(C) of [9, Theorem 0.1].

Since $V = \mathrm{H}_1(X, \mathbf{Q})$ carries a natural structure of $E$-vector space, the first complex homology group $V_{\mathbf{C}} = \mathrm{H}_1(X, \mathbf{C}) = \mathrm{H}_1(X, \mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{C}$ carries a structure of $E_{\mathbf{C}}$-module, and therefore splits into a direct sum

$$V_{\mathbf{C}} = \oplus_{a \in G} V_a.$$

Each $V_a$ is a $\mathbf{C}$-vector space of dimension $\dim_E V = n-1$.

There is a canonical Hodge decomposition ([3, chapter 1], [1, pp. 52–53])

$$V_{\mathbf{C}} = \mathrm{H}_1(X, \mathbf{C}) = \mathrm{H}^{-1,0}(X) \oplus \mathrm{H}^{0,-1}(X)$$

where $\mathrm{H}^{-1,0}(X)$ and $\mathrm{H}^{0,-1}(X)$ are mutually "complex conjugate" $\dim(X)$-dimensional complex vector spaces. This splitting is $E$-invariant, and $\mathrm{H}^{-1,0}(X)$ and $\mathrm{Lie}(X)$ are canonically isomorphic as $E_{\mathbf{C}}$-modules. In particular,

$$\dim_{\mathbf{C}} \mathrm{H}^{-1,0}(X)_a = \dim_{\mathbf{C}} \mathrm{Lie}(X)_a = n_a.$$

Let $\mathfrak{f}_H^0 = \mathfrak{f}_{H,Z}^0 : V_{\mathbf{C}} \to V_{\mathbf{C}}$ be the $\mathbf{C}$-linear operator such that

$$\mathfrak{f}_H(x) = -x/2 \quad \forall\ x \in \mathrm{H}^{-1,0}(X); \quad \mathfrak{f}_H^0(x) = x/2 \quad \forall\ x \in \mathrm{H}^{0,-1}(X).$$

Since the Hodge decomposition is $E$-invariant, $\mathfrak{f}_H^0$ commutes with $E$. Therefore, each $V_a$ is $\mathfrak{f}_H^0$-invariant. It follows that the linear operator $\mathfrak{f}_H^0 : V_a \to V_a$ is semisimple and its spectrum lies in the two-element set $\{-1/2, 1/2\}$. The multiplicity of eigenvalue $-1/2$ is $n_a = \dim_{\mathbf{C}} \mathrm{H}^{-1,0}(X)_a$, while the multiplicity of eigenvalue $1/2$ is $\dim_E V - n_a$. Clearly, the complex conjugate of $a \in \mathrm{Gal}(E/\mathbf{Q}) = (\mathbf{Z}/q\mathbf{Z})^*$ is $\bar{a} = q - a$. It is known ([1], [2]) that

$$n_a + n_{\bar{a}} = \dim_E V. \tag{2}$$

This implies that the multiplicity of the eigenvalue $1/2$ is $n_{\bar{a}}$.

The Hodge Lie algebra hdg of $X$ is a reductive $\mathbf{Q}$-Lie subalgebra of $\mathrm{End}_{\mathbf{Q}}(V)$. Its natural representation in $V$ is completely reducible and its centralizer in $\mathrm{End}_{\mathbf{Q}}(V)$ coincides with $\mathrm{End}^0(X) = E$. Moreover, its complexification

$$\mathrm{hdg}_{\mathbf{C}} = \mathrm{hdg} \otimes_{\mathbf{Q}} \mathbf{C} \subset \mathrm{End}_{\mathbf{Q}}(V) \otimes_{\mathbf{Q}} \mathbf{C} = \mathrm{End}_{\mathbf{C}}(V_{\mathbf{C}})$$

contains $\mathfrak{f}_H^0$ [8, Sect. 3.4]. Recall that $\mathrm{hdg} = \mathfrak{c} \oplus \mathrm{hdg}^{ss}$, with $\mathfrak{c}$ being the center of hdg and $\mathrm{hdg}^{ss} = [\mathrm{hdg}, \mathrm{hdg}]$ the semisimple part. Let $\mathfrak{c}_{\mathbf{C}} := \mathfrak{c} \otimes_{\mathbf{Q}} \mathbf{C}$ be the complexification of $\mathfrak{c}$ and $\mathrm{hdg}^{ss}_{\mathbf{C}} := \mathrm{hdg}^{ss} \otimes_{\mathbf{Q}} \mathbf{C}$ the complexification of $\mathrm{hdg}^{ss}$. Clearly, $\mathrm{hdg}^{ss} \subset \mathfrak{sl}_E(V)$, and thus

$$\mathrm{hdg}^{ss}_{\mathbf{C}} \subset \mathfrak{sl}_{E_{\mathbf{C}}}(V_{\mathbf{C}}) = \oplus_{a \in G} \mathfrak{sl}_{\mathbf{C}}(V_a).$$

We write $\mathrm{hdg}^{ss}_a$ for the image of projection $P_a : \mathrm{hdg}^{ss}_{\mathbf{C}} \to \mathfrak{sl}_{\mathbf{C}}(V_a)$. Clearly, each $\mathrm{hdg}^{ss}_a$ is a semisimple complex Lie subalgebra of $\mathfrak{sl}_{\mathbf{C}}(V_a)$.

**Remark 8.** Let us decompose $f_H^0$ as $f + f'$ with $f' \in \mathfrak{c}_{\mathbf{C}}$ and $f \in \mathrm{hdg}^{ss}_{\mathbf{C}}$. By [9, Remark 3.2], the natural representation $V_a$ of $\mathrm{hdg}^{ss}_a$ is simple for all $a \in G$. It follows from Schur's Lemma that when restricted to each $V_a$, $f'$ coincides with multiplication by scalar $c_a \in \mathbf{C}$. Therefore, $\mathrm{hdg}^{ss}_{\mathbf{C}}$ contains an operator (namely, $f$) whose restriction on each $V_a$ is diagonalizable with at most two eigenvalues: $-1/2 - c_a$ of multiplicity $n_a$ and $1/2 - c_a$ of multiplicity $n_{\bar{a}} = \dim_E V - n_a$.

**Lemma 9.** *Let the assumptions be the same as in Theorem 1. There exists an* $a \in G = (\mathbf{Z}/q\mathbf{Z})^*$ *such that* $\mathrm{hdg}^{ss}_a = P_a(\mathrm{hdg}^{ss}_{\mathbf{C}})$ *coincides with* $\mathfrak{sl}_{\mathbf{C}}(V_a)$.

*Proof.* The idea is to combine Remark 7, 8 together with Lemma 3.3 of [9]. This result is already contained in the proof of [9, Theorem 3.4], where we note that the assumption $n > q$ in [9, Theorem 3.4] is not used for this particular step of the proof. □

Notice that this is the place where assumptions (A)(B)(C) in Theorem 1 are used, since we need to make sure that there exists $a \in G$ such that $n_a$ and $\dim_E V$ are relative prime in order to apply Lemma 3.3 of [9].

Let $h : (\mathbf{Z}/q\mathbf{Z})^* \to \mathbf{R}$ be the function such that for all $1 \leq a \leq q-1$ with $\gcd(a, q) = 1$,

$$h(a) = \left(\frac{\dim_E V}{2} - n_a\right)^2 = \left(\frac{n-1}{2} - \left[\frac{na}{q}\right]\right)^2. \tag{3}$$

By (2), $n_a + n_{\bar{a}} = \dim_E V$, so $h(a) = h(\bar{a}) = h(q-a)$, which is also easy to check directly from (3). The function $h$ is non-increasing on the set of integers

$$[1, q/2]_{\mathbf{Z}} := \{a \mid 1 \leq a \leq q/2, \gcd(a, p) = 1\}.$$

By Remark 3, we have $4 \leq n < q$. In particular, $[n/q] = 0$. On the other hand, let $t$ be the maximal element of $[1, q/2]_{\mathbf{Z}}$. Then $t \neq 1$ and $[nt/q] \neq 0$. It follows that $h$ is not a constant function.

**Lemma 10.** *Let the assumption be the same as Theorem 1. Let* $(a, b) \in G^2$ *be a pair such that* $h(a) \neq h(b)$. *Then* $P_{a,b}(\mathrm{hdg}^{ss}_{\mathbf{C}}) = \mathfrak{sl}_{\mathbf{C}}(V_a) \oplus \mathfrak{sl}_{\mathbf{C}}(V_b)$.

*Proof.* By (3),

$$h(a) - h(b) = (n_a - n_b)(\dim_E V - n_a - n_b).$$

So $h(a) \neq h(b)$ if and only if $n_a \neq n_b$ and $n_a \neq \dim_E V - n_b$. Let $\mathfrak{k}^{ss} = P_{a,b}(\mathrm{hdg}^{ss}_{\mathbf{C}})$. By Lemma 9 and part (i) of Lemma 5, both projections $\mathfrak{k}^{ss} \to \mathfrak{sl}_{\mathbf{C}}(V_a)$ and $\mathfrak{k}^{ss} \to$

$\mathfrak{sl}_{\mathbf{C}}(V_b)$ are surjective. By Remark 8, $P_{a,b}(f)$ is a semisimple element of $\mathfrak{k}^{ss} \subseteq \mathrm{End}_{\mathbf{C}}(V_a) \oplus \mathrm{End}_{\mathbf{C}}(V_b)$ such that $P_{a,b}(f)$ acts on $V_a$ with (at most) 2 eigenvalues of multiplicities $n_a$ and $\dim_E V - n_a$ respectively, and similarly for $b$. Lemma 10 follows by setting $d = 2$ in [9, Lemma 3.6]. Last, we point out that the assumption that the multiplicities $a_i$ are positive in [9, Lemma 3.6] is not used in its proof, so the lemma applies to the case that $n_a$ or $n_b$ is zero, which may happen if $n < q$. $\square$

*Proof of Theorem 1.* As remarked at the end of Section 2, Theorem 1 follows if we show that the conditions (I) and (II) of Lemma 6 holds for $\mathfrak{k} = \mathrm{hdg}^{ss}$. Condition (I) holds by Lemma 9. To show that Condition (II) holds, by Lemma 10 it is enough to prove that for each $(a, b) \in G^2$ with $a \neq b$ and $a \neq \bar{b}$, there exists $x \in G$ such that $h(xa) \neq h(xb)$. Suppose that this is not the case, then there exists a pair $(a, b)$ such that $h(xa) = h(xb)$ for all $x \in G$. Without loss of generality, we may and will assume that $b = 1 \in (\mathbf{Z}/q\mathbf{Z})^*$, thus $a \neq \pm 1$. It follows that $h(xa) = h(x)$ for all $x \in (\mathbf{Z}/q\mathbf{Z})^*$. Since $h$ is not a constant function, such an $a$ does not exists by Lemma 11 of next section. Contradiction. $\square$

## 4. Arithmetic Results

Throughout this section, $G = (\mathbf{Z}/q\mathbf{Z})^*$. For each $a \in G$, let $\theta_a : G \to G$ be the translation map: $b \mapsto ab$. A function $h : G \to \mathbf{R}$ is said to be *even* if $h \circ \theta_{-1} = h$. For any $x \leq y \in R$, we write $[x, y]_{\mathbf{Z}}$ for the set of integers $\{i \mid x \leq i \leq y, \gcd(i, p) = 1\}$.

**Lemma 11.** *Let $h : (\mathbf{Z}/q\mathbf{Z})^* \to \mathbf{R}$ be an even function that's monotonic on $[1, q/2]_{\mathbf{Z}}$. If $h \circ \theta_a = h$ for some $a \in (\mathbf{Z}/q\mathbf{Z})^*$ and $a \neq \pm 1$, then $h$ is a constant function.*

*Proof.* We prove the Lemma in seven steps.

**Step 1.** Let $\langle \pm a \rangle$ be the subgroup of $(\mathbf{Z}/q\mathbf{Z})^*$ generated by $a$ and $-1$. Clearly $h \circ \theta_b = h$ for any $b \in \langle \pm a \rangle$ since $h \circ \theta_a = h$ and $h$ is even. In particular, this holds true for the maximal element $b_{\max}$ in the set in $\langle \pm a \rangle \cap [1, q/2]_{\mathbf{Z}}$. If $b_{\max} = 1$, the group $\langle \pm a \rangle$ is necessarily $\{\pm 1\}$. Therefore, it is enough to prove that $h$ being nonconstant implies that $b_{\max} = 1$. So with out lose of generality, we assume that $a = b_{\max}$ throughout the rest of the proof. Notice that if $a \neq 1$, then $2a^2 > q$, for otherwise it contradicts the maximality of $a$.

**Step 2.** Lemma 11 holds if $p = 2$.

Every even function on $(\mathbf{Z}/q\mathbf{Z})^*$ is constant if $q$ is 2 or 4 so we assume that $q = 2^r \geq 8$. The group $(\mathbf{Z}/2^r\mathbf{Z})^*$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{r-2}\mathbf{Z}$, where the factor $\mathbf{Z}/2\mathbf{Z}$ is generated by $-1$. Let us assume that $\langle \pm a \rangle$ has order $2^s$. Since $\langle \pm a \rangle \supseteq \langle \pm 1 \rangle$, it follows that $\langle \pm a \rangle \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{s-1}\mathbf{Z}$. In particular, if $\langle \pm a \rangle \neq \langle \pm 1 \rangle$, then $\mathbf{Z}/2^{s-1}\mathbf{Z}$ is nontrivial, therefore $\langle \pm a \rangle$ contains 3 elements of order two. But there are exactly 3 elements of order two in $(\mathbf{Z}/q\mathbf{Z})^* : -1, 2^{r-1} - 1, 2^{r-1} + 1$. Hence $\langle \pm a \rangle$ contains all the above elements of order 2. So $a = 2^{r-1} - 1$ since it is the largest element in $[1, q/2]_{\mathbf{Z}}$. Therefore,

$$h(q/2 - 1) = h(2^{r-1} - 1) = h(a) = (h \circ \theta_a)(1) = h(1).$$

Since $h$ is monotonic on $[1, q/2]_{\mathbf{Z}}$, the above equality implies that $h$ is constant on $[1, q/2]_{\mathbf{Z}}$ and therefore a constant function.

**Step 3.** Let $p$ be an odd prime. Lemma 11 holds if either $a$ is even, or $a$ is odd and $3a \geq q$.

It is enough to prove that if $a \neq 1$, then $h(1) = h((q-1)/2)$. Since $h(1) = (h \circ \theta_a)(1) = h(a)$, by monotonicity $h$ is constant on $[1, a]_{\mathbf{Z}}$. Therefore it is enough to find $b$ such that $h((q-1)/2) = h(b)$ and $b \in [1, a]_{\mathbf{Z}}$.

First, let's assume that $a = 2b$ is even. Then

$$a \cdot \frac{q-1}{2} = (q-1)b \equiv -b \mod q.$$

So $h((q-1)/2) = h(a(q-1)/2) = h(-b) = h(b)$. Clearly $b = a/2$ lies in $[1, a]_{\mathbf{Z}}$.

Next, assume that $a$ is odd. Then

$$a \cdot \frac{q-1}{2} = \frac{qa-a}{2} \equiv \frac{q-a}{2} \pmod q.$$

So $h((q-1)/2) = h((q-a)/2)$. Let $b = (q-a)/2$. When $3a \geq q$, we have $b = (q-a)/2 \leq a$ hence $b$ lies in $[1, a]_{\mathbf{Z}}$ as desired.

**Step 4.** Lemma 11 holds if $p = 3$.

When $p$ is odd, $(\mathbf{Z}/p^r\mathbf{Z})^*$ is cyclic of order $\varphi(p^r) = (p-1)p^{r-1}$. For $p = 3$,

$$(\mathbf{Z}/3^r\mathbf{Z})^* \cong \mathbf{Z}/(2 \cdot 3^{r-1})\mathbf{Z} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3^{r-1}\mathbf{Z}.$$

In particular, if $q \geq 9$, $(\mathbf{Z}/q\mathbf{Z})^*$ contains a unique subgroup of order 3 which is generated by $3^{r-1}+1$. If the order of $\langle \pm a \rangle$ is coprime to 3, then $\langle \pm a \rangle$ is necessarily $\{\pm 1\}$, which leads to an contradiction. If the order of $\langle \pm a \rangle$ is divisible by 3, then $q \geq 9$ and $\langle \pm a \rangle$ contains $3^{r-1}+1$. By assumption on the maximality of $a$ we must have $a \geq 3^{r-1}+1$ and hence $3a > q$.

**Step 5.** Assume that both $p$ and $a$ are odd, $p \neq 3$ and $3a < q$. Lemma 11 holds if $7a \geq q$.

Since $p \neq 3$, $(q-3)/2$ lies in $[1, q/2]_{\mathbf{Z}}$. It is enough to prove that $a \neq 1$ implies that $h(1) = h((q-3)/2)$. Indeed, it follows from the proof of Step 3 that $h((q-1)/2) = h((q-a)/2)$. But if $a \neq 1$ then $a \geq 3$ so $(q-a)/2 \leq (q-3)/2$. If we prove that $h$ is constant on $[1, (q-3)/2]_{\mathbf{Z}}$, then $h((q-1)/2) = h((q-a)/2) = h(1)$ and it follows that $h$ is a constant function.

By our assumption $3a < q$, so $(q-3a)/2$ lies in $[1, q/2]_{\mathbf{Z}}$. Notice that

$$a \cdot \frac{q-3}{2} \equiv \frac{q-3a}{2} \mod q.$$

We see that $h((q-3)/2) = h((q-3a)/2)$. Since $h$ is constant on $[1, a]_{\mathbf{Z}}$, the inequality $h(1) \neq h((q-3)/2)$ would imply that $a < (q-3a)/2$, or equivalently $5a < q$. In particular, $2a < q/2$. But $2 \in [1, a]_{\mathbf{Z}}$ since $p$ is odd and $a \geq 3$. So $h(2) = h(1)$, therefore $h(2a) = h(1)$ and $h$ is constant on $[1, 2a]_{\mathbf{Z}}$. But now by our assumption $7a \geq q$, or equivalently $2a \geq (q-3a)/2$, it follows that

$$h\left(\frac{q-3}{2}\right) = h\left(\frac{q-3a}{2}\right) = h(1).$$

**Step 6.** Assume that both $p$ and $a$ are odd, $p \neq 3, 5$ and $7a < q$. Lemma 11 holds.

Since $7a < q$ and $p \neq 5$, $(q-5a)/2$ lies in $[1, q/2]_{\mathbf{Z}}$. By similar argument as in Step 5, $h((q-5)/2) = h((q-5a)/2)$. We claim that now it is enough to show that $h(1) = h((q-5)/2)$. Indeed, by the proof of the Step 5, all we need to show is that $h(1) = h((q-3)/2)$, but since $a \geq 3$, then $(q-3a)/2 < (q-5)/2$. So $h$ being constant on $[1, (q-5)/2]_{\mathbf{Z}}$ implies that $h(1) = h((q-3a)/2) = h((q-3)/2)$.

Let $S$ be the set of all integers

$$S = \{b \mid b \geq 1, p \nmid b, (2b+1)a < q\}.$$

Clearly $1 \in S$ so $S$ is not empty. Let $x$ be the maximal element of $S$. By Step 1, $2a^2 > q$ so necessarily $x < a$. Since $h$ is constant on $[1, a]_{\mathbf{Z}}$, we must have $h(1) = h(x)$. Notice that $xa < q/2$ by assumption. So $h(ax) = h(x) = h(1)$ and it follows that $h$ is constant on $[1, ax]_{\mathbf{Z}}$. Assume that $h(1) \neq h((q-5)/2)$. It is necessary that $ax < (q-5a)/2$, or equivalently, $(2x+5)a < q$. But we can choose $x'$ from the two elements set $\{x+1, x+2\}$ such that $x'$ is coprime to $p$. It follows that $x' \in S$. This contradicts the maximality of $x$.

**Step 7.** Lemma 11 holds if $p = 5$.

If the order of $\langle \pm a \rangle$ is divisible by 5, then $\langle \pm a \rangle$ contains the unique subgroup of order 5 in $(\mathbf{Z}/5^r\mathbf{Z})^*$. In particular, $2 \cdot 5^{r-1} + 1 \in \langle \pm a \rangle$. It follows that $a > 2 \cdot 5^{r-1} + 1$ and therefore $3a > 5^r$. The Lemma holds by Step 3.

If the order of $\langle \pm a \rangle$ is coprime to 5. Then from the isomorphism

$$\mathbf{Z}/5^r\mathbf{Z} \cong \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/5^{r-1}\mathbf{Z},$$

we see that $\langle \pm a \rangle$ is has either order 2 or 4. If $\langle \pm a \rangle$ has order 2, then $\langle \pm a \rangle$ is necessarily $\langle \pm 1 \rangle$ and this leads to a contradiction. So we assume that $\langle \pm a \rangle$ has order 4 and $a$ is the unique element such that $1 < a < 5^r/2$ and $a^2 \equiv -1 \mod 5^r$. In particular, $a^2 + 1 \geq 5^r$. If $a$ is even then the Lemma holds by Step 3. In particular, this works for $q = p = 5$ since $a = 2$ in this case. We assume that $q \geq 25$ and $a$ is odd through out the rest of the proof. First we claim that $a \geq 7$. Indeed, If $q = 25$, then $a = 7$ by direct calculation; if $q > 25$, then $a > 7$ since $a^2 + 1 \geq q$. This implies that $(q-a)/2 \leq (q-7)/2$. Therefore, it is enough to prove that $h((q-7)/2) = h(1)$ since it then follows that $h((q-1)/2) = h((q-a)/2) = h(1)$. By Step 5 we may also assume that $7a < q$. It follows that $(q-7a)/2 \in [1, q/2]_{\mathbf{Z}}$ and $h((q-7)/2) = h((q-7a)/2)$.

Let $c = [q/a]$. Since $a^2 + 1 \geq q$ and $a < q/2$ we see that $2 \leq c \leq a$. Let $x = [c/2]$ if $[c/2]$ is not divisible by 5, and $x = [c/2] - 1$ otherwise. Notice that $a > x \geq \max\{1, (c-3)/2\}$ and $xa \leq q/2$ by our choice of $x$. It follows that $x \in [1, a]_{\mathbf{Z}}$ therefore $h(x) = h(1)$, and therefore $h(ax) = h(x) = h(1)$. So $h$ is constant on $[1, ax]_{\mathbf{Z}}$. If $h(1) \neq h((q-7)/2)$, we must have $xa < (q-7a)/2$, or equivalently, $(2x+7)a < q$. Then it follows that

$$\frac{q}{a} > 2x + 7 \geq 2\left(\frac{c-3}{2}\right) + 7 = c + 4 = \left[\frac{q}{a}\right] + 4,$$

which is absurd.

Lemma 11 is proved by combining all the above steps. □

## References

[1] P. Deligne, *Hodge cycles on abelian varieties* (notes by J.S. Milne). Lecture Notes in Math., vol. **900** (Springer-Verlag, 1982), pp. 9–100.

[2] B. Moonen, Yu.G. Zarhin, *Weil classes on abelian varieties.* J. reine angew. Math. **496** (1998), 83-92.
[3] D. Mumford,: Abelian varieties, Second edition. Oxford University Press, London, 1974.
[4] K. Ribet, *Galois action on division points of Abelian varieties with real multiplications.* Amer. J. Math. **98**, 751–804 (1976).
[5] K. Ribet, *Hodge classes on certain abelian varieties.* Amer. J. Math. **105** (1983), 523–538.
[6] D. Ulmer, Yu.G. Zarhin, *Rank of Jacobians in towers of function fields*, Math. Res. Lett. **17**(2010), No. **4**, 637–645.
[7] J. Xue, *Endomorphism algebras of Jacobians of certain superelliptic curves*, J. Number Theory, **131** (2011), 332–342.
[8] J. Xue, Yu.G. Zarhin, *Centers of Hodge groups of superelliptic Jacobians*, Transformation Groups, **15** (2010), no. **2**, 449–482.
[9] J. Xue, Yu.G. Zarhin, *Hodge groups of certain superelliptic Jacobians*, Math. Res. Lett. **17** (2010), no.**2**, 371–388.
[10] Yu.G. Zarhin, *Weights of simple Lie algebras in the cohomology of algebraic varieties.* Izv. Akad. Nauk SSSR Ser. Mat. **48** (1984), 264–304; Math. USSR Izv. **24** (1985), 245 - 281.
[11] Yu.G. Zarhin, *Hyperelliptic jacobians without complex multiplication.* Math. Res. Letters **7** (2000), 123–132.
[12] Yu.G. Zarhin, *Very simple* 2*-adic representations and hyperelliptic jacobians.* Moscow Math. J. **2** (2002), issue 2, 403-431.
[13] Yu.G. Zarhin, *Cyclic covers, their Jacobians and endomorphisms.* J. reine angew. Math. **544** (2002), 91–110 .
[14] Yu.G. Zarhin, *The endomorphism rings of Jacobians of cyclic covers of the projective line.* Math. Proc. Cambridge Philos. Soc. **136** (2004), 257–267.
[15] Yu.G. Zarhin, *Endomorphism algebras of superelliptic Jacobians.* In: F. Bogomolov, Yu. Tschinkel (eds.) Geometric methods in Algebra and Number Theory, Progress in Math. **235**, 339–362, Birkhäuser, Boston Basel Berlin, 2005.
[16] Yu.G. Zarhin, *Superelliptic jacobians.* In: "Diophantine Geometry" Proceedings (U. Zannier, ed.), Edizioni Della Normali, Pisa 2007, pp. 363-390.
[17] Yu.G. Zarhin, *Endomorphisms of superelliptic jacobians.* Math. Z., **261** (2009), 691–707, 709.

National Center for Theoretical Sciences, Math. Division, Third General Building, National Tsing Hua University, No.101, Sec 2, Kuang Fu Road, Hsinchu, Taiwan 30043, Taiwan R.O.C.

*E-mail address*: `xue_j@math.cts.nthu.edu.tw`